SCIREA Journal of Mathematics

http://www.scirea.org/journal/Mathematics

November 29, 2016

Volume 1, Issue1, October 2016

RATIONAL POINTS ON ELLIPTIC CURVES; THE ULTIMATE SOLUTION OF THE MILLENIUM PRIZE PROBLEM; BSD-CONJECTURE

Lena J-T Strömberg

previously Department of Solid Mechanics, Royal Institute of Technology (KTH)

e-mail: lena_str@hotmail.com

Abstract

Rational points on elliptic curves are considered, in the formulation of BSD, and for nonlinear dynamical systems. Method used is the intersection with other curves, for a more general expression of an elliptic curve, known as an extended elliptic curve. It is found that there are elliptic curves with at most 3 rational solutions for certain rational values of parameters, c.f. Theorem 3.

Keywords: Elliptic Curves, Rational numbers, Number Theory, Millennium Prize Problem, ultimate solution, associated ellips, associated hyperbolic, cusp, Nonlinear Dynamics, Phase Portrait, Lorenz equations, aqua plane, Hamiltonian

1. INTRODUCTION

In the present context, the Birch and Swinnerton-Dyer conjecture as formulated in the Millennium setting, will be considered and notations from Clay Mathematics Institute's prize problem[1] are used. The conjecture addresses rational points on elliptic curves f(x,y)=0, i.e. the number of solutions (x,y) that are rational numbers. Elliptic curves occur at descriptions of motions, when time development of variables fulfils balance equations, e.g. balance of energy, and momentum. Such linear and nonlinear dynamic analysis, is the foundation of Hamiltonian Mechanics. For a linear harmonic oscillator, the ellipse or unit circle appears as a so-called Hamiltonian, and e.g. $x^2+y^2=1$. Integer points are the 'trivial' end points (x,y)=(0,1), (1,0).

Rational points are the integer points and 3/5, 4/5. With this exact consideration, there are a finite number of solutions for both integers and rational points. A graph of the function over the integers and the rationals is shown in Figure 1.

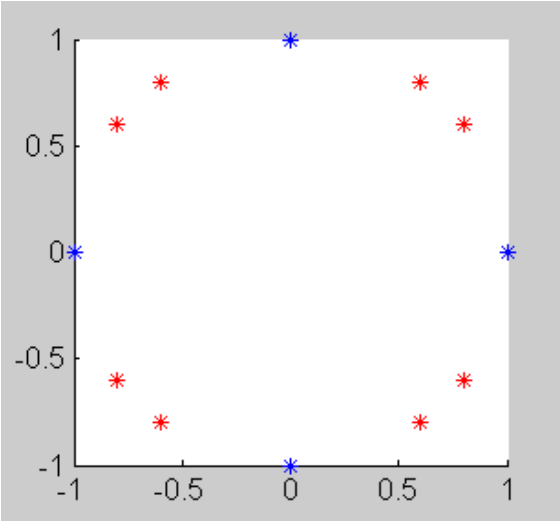

Figure 1. Rationals point on a circle

1.1 Elliptic curves

Conjecture specifies to determine rational solutions to elliptic curves in the Weierstrass form

$y^2= x^3 + ax + b$ …..(1)

Some properties and graphs of such curves are given in e.g. Wikipedia.

Cusp condition. Concerning the shape, the magnitude of the factor $4a^3/(27b^2)$ determines whether curve has a cusp.

2. ENGINEERING APPLICATION

The nonlinear dynamical model for aqua-plane[2], is revisited. Motion is described in terms of a Hamiltonian H, as a function of an angle ϕ, and an angular velocity $d_t\phi$.

The normalised Hamiltonian reads $H=H(\phi,d_t\phi)=(d_t\phi)^2+a_0\phi^2+a_1\phi^3-a_2\phi(d_t\phi)^2$

When damping is neglected, simulation is done for constant energy H, corresponding to initial velocity, that, if periodic motion, equals maximum velocity and determines eigenfrequency.

For largest a_1, the maximum positive angle will be small, and the acceleration is large at positive turning point, such that the negative velocity causes an 'escape from orbit' corresponding to a flip backwards. For moderate a_1, there is periodic motion, with larger maximum negative angle and slower acceleration and velocity at negative turning point, such that longer time 'is spent there'. For smaller H and largest a_1, behaviour is stable periodic motion as seen for the innermost circle, in Figure 2.

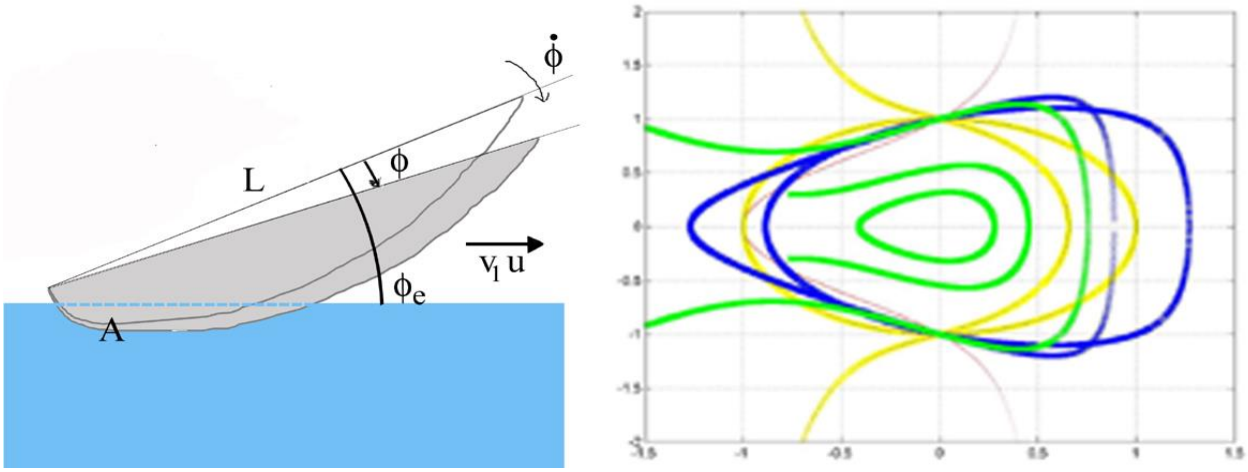

Figure 2. Phase portrait $d_t\phi$ versus ϕ for Hamiltonian H=1, and parameters $[a_0, a_1, a_2]$=[1,-0.3, 0.7], [1,0, 0], [1,0.3,1], [1,1,1], [1,2,-1], and H=0.3[1,1,1], H=0.1[1,1,1],from right at $(d_t\phi,\phi)$=(0,1.5), and diverging at ϕ=0.5; H=1[1,0, 2].

Behavior agrees with the motion of a natural existing mechanical system. This motivates the consideration of the curve

$H(-x,y)= y^2 + a_0x^2 - a_1x^3 - a_2xy^2$, as a basis, in the preliminaries of finding rational points.

Proposition 1: Function $y^2 = a_1x^3 -a_0x^2 + a_2xy^2+b$, describing the motion at aqua-plane, the side conditions (constraints) a_1=1 and, $y^2 =a_0/a_2x + a/a_2$, is an elliptic curve in the format (1).

Proof: Insertion and identification of parameters.

Definition 1: When a_1 is not equal to one, this will be denoted an *extended elliptic curve*.

Remark: When side condition $y^2 = a_0/a_2 x + a/a_2$, has rational solutions, the intersection points, can be rational.

3. RATIONAL POINTS ON THE ELLIPTIC CURVE.

Theorem *1:* The intersection with the scaled unit circle, provides rational points, on an extended elliptic curve $y^2=cx^3+dx+e$. Solutions are given by two equations for coefficients c,d,e. One such curve is given by c=1, d= -12, e =25.

Proof: Curve is rewritten as $y^2=x^2 (cx+d/x) +e$.

Dividing with parameter e, using a requirement (cx+d/x)=-1 and substitution of the two solutions for the circle (x,y)=(3/5, 4/5) and (x,y)=-(3/5, 4/5) gives two equations, which determine c and d.

A general format, could be derived by scaling the extended elliptic curve.

This is done by a transformation $x= \alpha\xi$, where α is rational and considering rational points in (ξ, y)-space. For the scaled curve, the intersection with an ellipse is considered.

Definition 2: When the end point x=0, is rational and also on the ellipse, this will be known as the *associated ellipse*.

Theorem 2: The extended elliptic curve $y^2=5/(r^3 b^{½})x^3 - 12b^{½}/(5r)x+b$ have rational solutions, provided that $b^{½}$ and r is rational.

Proof: Solutions are found as the intersections with the associated ellipse, with the method in proof of theorem 1.

Theorem 3: The elliptic curve $y^2=x^3 - 12/r^4 x+25/r^6$ have the rational solutions

$(x,y)=(3/r^2, 4/ r^3)$ and $(x,y)=(-4/r^2, 3/ r^3)$. These are shown in Figure 3.

Proof: Follows from Theorem 1 and 2, and elimination of b from requirement $5/(r^3 b^{½})=1$ for elliptic curve. These together with the trivial at zero gives that there are at most 3 solutions.

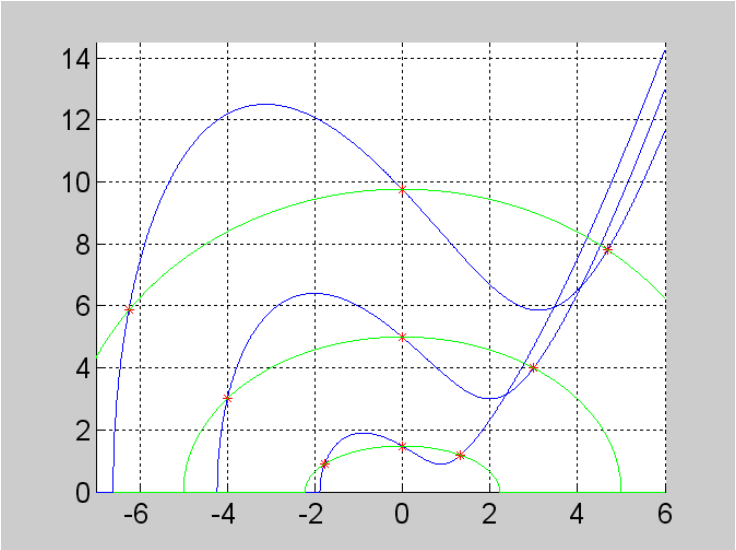

Figure 3. Elliptic curves and associated ellipses, r=0.8, 1, 1.5 from top

Supposition. The rational pairs $(x,y)=(-3/r^2, 4/ r^3)$ and $(x,y)=(4/r^2, 3/ r^3)$, are also on the ellipse. That these are not solution to an elliptic curve could probably be shown by reflexion, i.e. transformation $x=-x_s$.

3.1 Intersections with associated hyperbolic.

In conjunction with the associated ellipse, solutions that are intersections with an associated hyperbolic function will be sought. Derivation is similar to that of the associated ellipse. Hereby, it is found that

Theorem 4

The elliptic curve $y^2=x^3 - 11*3/5^3x+64/5^4$ have the rational solutions $(x,y)=(3/5, 2/5)$ and $(0,8/5^2)$

The elliptic curve $y^2=x^3 - 19*3/5^3x+64/5^4$ have the rational solutions $(x,y)=(-3/5, 2/5)$. and $(0,8/5^2)$

The curves and associated hyperbolic is shown in Figure 4 below. It is seen that the leftmost curve, dashed, has a cusp.

Remark. Curve can be scaled according to a/α^2, b/α^3 This follows from the transformation $x= \alpha\xi$, $y= \beta\eta$, and the requirement $\alpha^3=\beta^2$, to be an elliptic curve.

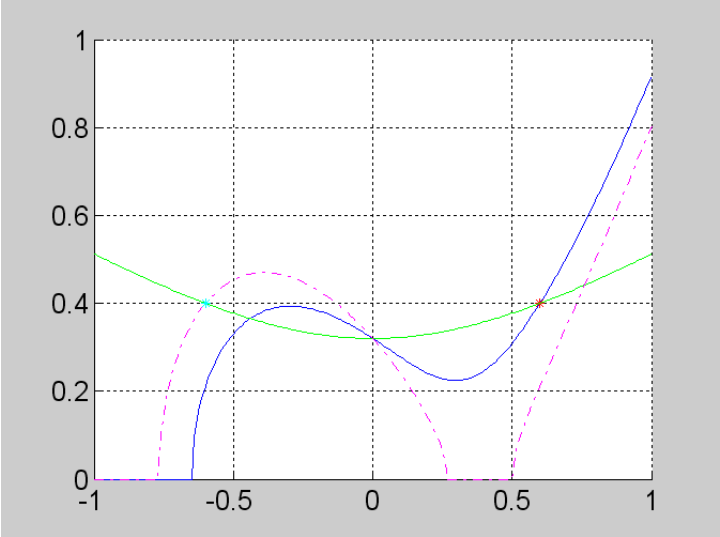

Figure 4. Associated hyperbolics and intersection points. One elliptic curve with a cusp.

With these preliminaries, a concluding theorem with the number of rational points will be formulated.

Theorem 5: The elliptic curve has at most 3 rational points for certain values of a, b, given in Theorem 3. For curves with a cusp, the rational points are given by Theorem 4, at most 2.

Proof: Elliptic curves can be written $y^2=x^2(x+a/x)+b$, where, x+a/x, is positive or negative and real. For the rational points, x+a/x, is rational. Hereby, every rational point on an elliptic curve is on an ellipse or hyperbola. Maximum number of rational points is equal to rational points of the associated ellipse/hyperbolic, at most 3, cf. Theorem3 and Theorm4.

4. CONNECTIONS TO A PROJECTION OF LORENZ EQUATIONS.

The 3-dim Lorenz equations are scaled and rewritten with constants with no dimension. With some assumptions, this format can be related to elliptic curves. When two of the variables in the Lorenz system are assumed constant, differential equations for the third can be derived. This will be called a static projection. Since Lorenz equation is a nonlinear systems, several solution will display. Static projection to one-dimensional systems gives

In x-direction $d_tx =\sigma(c-x)$ or $d_tx = -\sigma x+ \sigma\rho\beta\ x /(x^2+\beta)$

In y-direction $d_ty=-(y^3/\beta)+y(\rho-1)$

In z-direction $z=\rho-1$ or $d_tz =-\beta z$, or $d_tz=c-\beta(\rho-1)$

where c denotes an ('initial'-value-)constant, and σ,ρ, β -are the variables in Lorenz equation..

Some of these equations could be integrated, to a functional format. The right-most equation in x-direction will be related to an elliptic curve: Squaring, and a series expansion of right hand side, with linearisation and truncation, is an elliptic curve where 'y' is identified with $d_t x$. Also for y-direction, the square, and a truncated series expansion will have similarities with an elliptic curve.

Remark. For $\rho=-2$, the x-equation can be exactly integrated, and an (implicit) solution is given by $x(\beta+x^2/3)=C \exp(-3\sigma t)$, where C is an integration constant.

5. CONCLUSIONS

- The existence of rational pairs (x,y) on elliptic curves, were investigated. In this context, further correspondence between parameters in elliptic curve and a linear harmonic oscillator, mathematical pendulum, could be discussed, in terms of rational numbers, dimensions, & (multiples of) π.

- Extraction of impact force at bounce for the boat at aqua-plane, provides a compact formula, where points at the associated ellipse may be used.

- With a parametrisation of the associated ellipse and hyperb, relations to the exact explicit solution to Lorenz equation, (in terms of eg. time-constant σ) are obtained.

5. 1 Concluding Remarks

The scaling integers to rationals for the ellipsoidal, is what Andrew Wiles used, when solving Fermat's last theorem.

In the BSD-conjecture, in the format of the Millennium Prize problem, Andrew Wiles writes about a connection to the Riemann hypothesis, which is very difficult to understand. I also was told that the Mathematicians invented a new kind of numbers, which was not even intuitive.

The presentation above is a benchmark for a closure of the problem and an ultimate solution:

- it is well organised and relates to a linear case, defined by the associated ellipse or hyperbolic

- it harmonises with mechanics by a general Hamiltonian

- it is close to dynamical application; aquaplane and relates also to the well-known Lorenz' equations

Figure 5. Glastron speed boats, at aqua plane

REFERENCES

[1] The Birch and Swinnerton-Dyer conjecture, A Wiles, wikipedia, elliptic curves

[2] Continuum Mixture theory as an approach to Fluid-Structure Interaction, L Strömberg, IUTAM Symposium on Fluid-Structure Interaction in Ocean Engineering, Hamburg/Germany, July 23-27, 2007 and proc. NSCM 19, Lund, 2006.